SS

#16
12/30/03
AW

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	Eric D. Schneider, Michael J. Gustafson & Daniel J. Hagler
SERIAL NO.:	09/719,339
FILING DATE:	March 5, 2002
TITLE:	Method And Apparatus For Dealing With Data Corruption And Shared Disks In The Context Of Saving, Using And Recovering Data
EXAMINER:	Puente, Emerson C.
GROUP ART UNIT:	2184
ATTY. DKT. NO.:	20423-07924

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Declaration of Assignee's Attorney

I, Jeffrey Brill, hereby declare the following:

1. I am an attorney representing Symantec, Inc., the assignee of record of the above-referenced patent application.

2. Attached hereto as Exhibit A is a true and correct copy of one page from issued U.S. Patent 6,240,527 B1. The Tilios Operating System is described therein, at column 3 lines 5 - 42. According to Exhibit A, the Tilios Operating System was developed by the then assignee of the patent application that became U.S. Patent 6,240,527 B1.

4. Attached hereto as Exhibit B is a true and correct copy of a Substitute PTO-1449 Form, submitted to the U.S.P.T.O. during the prosecution of the patent application that became U.S. Patent 6,240,527 B1. According to Exhibit B, Tilios was offered for sale "around 1987."

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true.

9/15/03
Date

Jeffrey Brill
Registration Number 51,198

20423/07924/DOCS/1373698.1

relevant to the present invention other than being an option to use in conjunction with the present invention to provide means for recovery from both physical disk drive failures as well as undesired changes.

The Tilios Operating System was developed several years ago by the assignee hereof. It provided for securing a disk's state and then allowing the user to continue on and modify it. The operating system maintained both the secured and current states. Logging of keystrokes was performed so that in the event of a crash, where the current state is lost or becomes invalid, the disk could easily revert to its secured state and the log replayed. This would recover all disk information up to the time of the crash by, for example, simulating a user editing a file. The secured disk image was always available along with the current so that information could be copied forward in time—i.e., information saved at the time of the securing backup could be copied to the current state.

The Tilios Operating System could perform a more rapid backup because all the work was performed on the disk (e.g., there was no transfer to tape) and techniques were used to take advantage of the incremental nature of change (i.e., the current and secured states typically only had minor differences). Nonetheless, the user was still faced with selecting specific times at which to secure (backup) and the replay method for keystrokes was not entirely reliable for recreating states subsequent to the backup. For example, the keystrokes may have been commands copying data from a floppy disk or the Internet, both of whose interactions are beyond the scope of the CPU and disk to recreate.

Simply creating a backup a file by making a copy of a file under a new name, typically changing only a file's extension (e.g., "abc.doc" is copied to "abc.bak") has been a long standing practice. In the event the main file (abc.doc) is corrupted or lost, one can restore from the backup (abc.bak). This process is much the same as doing a selective tape backup and carries the issues of managing the backups (when to make, when to discard, etc.).

In summary, a RAID system only deals with backup in the context of physical drive failures. Tape, WORM, Tilios, and file copies also address backup in the context of recovering changed (lost) information.

No Specific Backup Request or Time

The traditional backup process involves stopping at a specific time and making a duplicate copy of the disk's information. This involves looking at the entire disk and making a copy such that the entire disk can be recreated or specific information recalled. This process typically involves writing to a tape. Alternatively, a user may backup a specific set of files by creating duplicates that represent frozen copies from a specific time. It is assumed the originals will go on to be altered. This process typically involves creating a backup file on the same disk drive with the original. Note that a "disk" may actually be one or more disk drives or devices acting in the manner of a disk drive (storage means).

In both of these cases the user must make a conscious decision to make a backup. In the second case a specific application, like a text editor, may keep the last few versions of a file (information). However, this can lead to wasted disk space as ultimately everything is duplicated long after files have stabilized. In other words, while working on a document a user may likely want to revert to a prior version, but once finished and years later, it is very unlikely the user would care to re-visit the last state before final.

The technology of the present invention seeks to eliminate the need to pause and make backups or decide which files should be backed up in the context of short term information recovery. That is, recovering information that was known reasonably recently as opposed, for example, to recovering information that has been lost for a long period of time.

Backup of a Disk's Directory is Important

Another situation where information recovery is very important is when the directory system for a disk, which identifies what and where files are located on disk, gets corrupted. This occurs, for example, due to a system crash during the directory's update or due to a bug in the operating system or other utility. In either case, losing the directory of a disk's contents results in losing the referenced files, even though they still exist on the disk. In this case the information the user wants to restore is the disk's directory.

A final example of why a user would want to revert to a backup is when the operating system gets corrupted (the executable or data files that are essential to run a computer) due, for example, to installing new software or device drivers that don't work.

Clearly there are many reasons a user might want to go back in time in the context of information being manipulated on a computer's disk. Traditional backups offer recovery to the time of the backup. However, these system-wide backups are limited in frequency due to the amount of time required to scan the disk and duplicate its contents. In other words, it is not feasible to backup an entire disk every few minutes as this would require significant pauses in operation and an enormous amount of storage. Keeping historical copies of files as they progress in time has the drawback of eventually forcing the user to manage the archives and purge copies in order to avoid overflowing the disk. Obviously, one cannot keep a backup of all files on a disk whenever they are changed for all of time without requiring an unlimited disk, which does not exist.

One approach to retaining discarded data on a more or less continuous basis is described in U.S. Pat. No. 5,325,519, entitled "Fault Tolerant Computer with Archival Rollback Capabilities", to Long et al. ("'519 patent"). The '519 patent discloses a storage device which includes processing circuitry for detecting access requests to alter data in respective locations of a storage device, and, prior to executing such requests, storing the data in such locations in an audit partition region of the storage device. The device of the '519 patent can subsequently restore the data retained in the audit partition region to its previous location on the device, and thereby return the storage device to a previous state. The device and approach of the '519 patent, however, inherently introduces delays in writing data to the storage device. In some cases, these delays may make it infeasible to use this technology. Therefore, there remains a need for a more fast, flexible and dynamic way to retain historical information in a computer system.

SUMMARY OF THE INVENTION

The present invention is a method and apparatus for disk based information recovery in computer systems. This applies to all types of computer systems that utilize one or more hard disks (or equivalent), where the disks represent a non-volatile storage system or systems. Such types of computers may be, but are not limited to, personal computers, network servers, file servers, or mainframes. The invention stipulates using the otherwise unused pages or special dedicated pages on a hard disk in a circular fashion to store the recent original states of information on the disk that is altered. Collectively these extra pages represent a history buffer. These history pages can be intermixed with the OS's data and thus the present invention relies on re-mapping of

Exhibit B

Form 1449*	Atty. Docket No.: 749.008US3	Serial No. Unknown
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary)	Applicant: Eric D. Schneider et al.	
	Filing Date: Herewith	Group: Unknown

U.S. PATENT DOCUMENTS

**Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
	5,297,258	03/22/1994	Hale, et al.			
	5,325,519	06/28/1994	Long, D.W., et al.	395	575	10/18/91
	5,331,646	07/19/1994	Krueger, et al.	371	40.1	05/08/92
	5,339,406	08/16/1994	Carney, M.W., et al.	395	575	04/03/92
	5,487,160	01/23/1996	Bemis	395	441	12/04/92
	5,524,205	06/04/1996	Lomet, et al.	395	182.14	04/21/93
	5,557,770	09/17/1996	Bhide, et al.			
	5,604,853	02/18/1997	Nagashima	395	803	05/18/92
	5,604,862	02/18/1997	Midgely, et al.	395	182.04	03/14/95
	5,640,561	06/17/1997	Satoh, et al.	395	618	06/06/95
	5,659,747	08/19/1997	Nakajima, S.	395	651	04/22/93

FOREIGN PATENT DOCUMENTS

**Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes	No

OTHER DOCUMENTS

**Examiner Initial	**Examiner(Including Author, Title, Date, Pertinent Pages, Etc.)
	"Tilios Secure Filing system - included in Applicants' application.", Offered for Sale around 1987., 1 Page.
	Castelletto, et al., "DB2 for VSE & VM Archiving and Recovery", IBM VSE/ESA, 1-18 (1996)
	Robinson, J.T., "Analysis of Steady-State segment storage utilizations in a log-structured file system with least-utilized segment cleaning", IBM Research Division, T. J. Watson Research Center, pp. 29-32.

Examiner	Date Considered

*Substitute Disclosure Statement Form (PTO-1449)

**EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.